Fuentes y medios de prueba electrónicos, dotación de seguridad jurídica a los documentos electrónicos

Diego Alejandro Gutiérrez Martin[*,**]
Universidad Católica de Colombia

Resumen

Mediante este trabajo se busca identificar y encontrar posibles soluciones a un problema que a vistas de futuro puede ser perjudicial en el proceso de documentación y disponer de herramientas para proporcionar seguridad jurídica a los documentos electrónicos, del mismo modo, examinar muy detalladamente cómo está estructurado el marco legal que garantiza la seguridad jurídica de los documentos electrónicos en Colombia. Actualmente contamos con herramientas electrónicas que nos facilitan la redacción de documentos y guardar estos mismos en equipos electrónicos o redes empresariales. Pero alguna vez nos hemos preguntado ¿Esta documentación privada está segura? ¿Es posible que sea robada o plagiada?

Como expresa Rendón (2009), se ve la necesidad "de crear nuevas formas, modelos, instrumentos o directrices, que permitan salvaguardar y garantizar la confidencialidad y autenticidad de los documentos electrónicos" (p. 1). Así mismo, verificar que medidas han sido propuestas y que no han sido aplicadas para la mitigación de la problemática presente, por lo tanto, los documentos electrónicos son:

> Los documentos electrónicos se han vuelto un reto para la seguridad jurídica, muchos autores indican que el uso de nuevas tecnologías a traído beneficios, teniendo en cuenta que ha sido un reto ya que para opinión de algunos aún estamos

---

[*] Artículo de investigación presentado como requisito para optar al título de Abogado de la Universidad Católica de Colombia, bajo la asesoría del doctor Marco Emilio Sánchez Acevedo, Abogado, especialista en Derecho Constitucional y Administrativo, Master en Ciberseguridad y Ciberdefensa, Master en Derecho Administrativo y Doctor en derecho.

[**] Estudiante en proceso de grado de la Facultad de Derecho de la Universidad Católica de Colombia, identificado con código estudiantil 2111319 y correo electrónico dagutierrez19@ucatolica.edu.co

> inmersos en la cultura del papel; sin embargo, al derecho le compete armonizar la necesidad de permitir la utilización eficaz de las nuevas tecnologías de la información con la necesidad de tutelar la confianza de las personas en la autenticidad y seguridad de los documentos generados y transmitidos electrónicamente (Díaz García, 2010, p. 2).

El uso de las nuevas tecnologías ha llevado a la obligación de estar atentos a estos cambios, aunque el sistema antiguo de archivo, como las bibliotecas y gestión documental física sean atractivas; es necesario estar al día y responder a los retos de la sociedad, siendo obligación para aquellos que trabajan en la rama del derecho a dar respuesta oportuna y adecuada a las preocupaciones que surjan del tema, así como dar soluciones eficaces.

Palabras Claves: Documentos electrónicos, Seguridad informática, Seguridad jurídica, prueba electrónica.

Abstract

This work seeks to identify and find possible solutions to a problem that, in the future, may be detrimental in the documentation process and to have tools to provide legal certainty to electronic documents, in the same way, to examine in detail how the document is structured. legal framework that guarantees the legal security of electronic documents in Colombia. Currently we have electronic tools that make it easier for us to write documents and save them on electronic equipment or business networks. But have we ever wondered if this private documentation is safe? Could it be stolen or plagiarized?

As Rendón (2009) expresses, there is a need to create new forms, models, instruments or guidelines that allow safeguarding and guaranteeing the confidentiality and authenticity of electronic documents, as well as verifying which measures have been proposed and have not been applied. for the mitigation of the current problem, therefore, the electronic documents are:

Electronic documents have become a challenge for legal security, many authors indicate that the use of new technologies has brought benefits, taking into account that it has been a challenge since in the opinion of some we are still immersed in the culture of paper, without However, it is up to the law to harmonize the need to allow the effective use of new information technologies with the need to protect people's trust in the authenticity and security of documents generated and transmitted electronically (Díaz García, 2010, p. 2).

The use of new technologies has led to the obligation to be aware of these changes, although the old filing system, such as libraries and physical document management, are attractive; It is necessary to be up-to-date and respond to the challenges of society, being an obligation for those who work in the field of law to give a timely and adequate response to the concerns that arise on the subject, as well as to provide effective solutions.

Key Words: Electronic documents, Computer security, Legal security, electronic proof.

Sumario

7.5. Ley 906 de 2004. 7.6. Artículo 242-Prueba documental. 7.7. Decreto 2364de 2012. Conclusión. Referentes bibliográficos.

Introducción

El tema de seguridad jurídica de los documentos electrónicos es muy extenso y con opiniones muy retrógradas por la desconfianza al uso de nuevas tecnologías, a pesar de la existencia de la informática, en el campo del derecho se ha utilizado tradicionalmente los documentos como prueba escrita, trayendo esto como consecuencia la acumulación de archivos que con el pasar del tiempo puede ser perdida de información relevante ya que los documentos físicos pueden sufrir cambios por cuestiones de sistema de archivado. Formentín (2013) afirma:

> El comercio electrónico genera incertidumbres derivadas de la misma naturaleza de los medios a través de los que este comercio se desenvuelve, y que plantean problemas de autenticación, integridad, rechazo y confidencialidad de las comunicaciones. Mientras desde el punto de vista técnico existen ya medios e instrumentos para solventar estos últimos problemas, desde el punto de vista jurídico, el estado actual de las leyes presenta todavía importantes incertidumbres que generan dudas importantes sobre la validez y eficacia de las transacciones electrónicas (p. 112).

Ahora bien, entrando en detalles, el comercio ha tomado gran posición “en el campo de la prueba electrónica, digital o incluso virtual y la misma goza de aceptación entre comerciantes, clientes de bancos, entidades financieras, compañías aseguradoras, de tarjetas de crédito y otras” (Jovel Sánchez, 2003, p. 42). Las transacciones realizadas por este tipo de comercios se llevan a cabo sin tener que crear o producir documentos físicos, minimizando gastos en papelería requerida, sin embargo, si se utilizan medios electrónicos es importante preguntarse si existen regulaciones jurídicas o mecanismos que puedan mantener segura la información que estos tipos documentos suministran.

Algunos autores exponen el significado de la inclusión de las nuevas tecnologías en la rama jurídica y los cambios significativos que esta produce. Becerra (2015) afirma:

> En primera medida, uno de los retos contemporáneos de la teoría de los derechos consiste en la explicación de las transformaciones que sufren tanto los derechos como sus concepciones en la era digital. Estos cambios, incluso, no solo plantean la existencia de nuevos derechos, como la inclusión digital, sino que ponen al límite la teoría liberal de los derechos en asuntos como la determinación de la titularidad de los sujetos, y desde, luego la fijación de las obligaciones y de los obligados que de allí se desprende (p. 197).

Es así como exponen que se deben realizar cambios en el derecho que exponga las medidas de usos de nuevas tecnologías. Becerra (2015) afirma:

> A su vez, Internet está pasando o ha pasado ya a ser esencial para la vida. Es un instrumento indispensable para ejercer libertades (expresión, información, asociación) y derechos participativos y sociales (educación, cultura, etc.). Puede ser un vehículo para mejorar la igualdad de oportunidades y la generalización de servicios de los poderes públicos que antes eran casi inimaginables. Es por ello que está emergiendo la consideración de que el acceso a Internet es un derecho fundamental autónomo de última generación. Pero también sería un viejo derecho esencialmente negativo, en la órbita de la libertad de expresión e información, que garantiza que el Estado no ponga barreras o censure el acceso mismo a la red y a sus contenidos (p. 197).

Concluyendo con lo mencionado en los anteriores párrafos, en donde se puede observar que uno de los nuevos retos contemporáneos en las teorías del derecho es la incursión de la era digital, por lo tanto, el internet se está volviendo un elemento esencial en esta era. Becerra (2015) afirma:

> En cuanto a la publicación de contenidos por parte de la administración y su marco de responsabilidad, es necesario determinar el cumplimiento o cumplimiento defectuoso de los principios y requerimientos legales de seguridad de la información, así como de los controles de seguridad impuestos en el nivel reglamentario. El cumplimiento de la reglamentación y de las normas técnicas por las administraciones incorpora un elemento adicional de examen en temas de la posible responsabilidad de la administración, en especial a la luz de incidentes que no se hubieran podido prever o evitar según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de su producción. Son de aplicación los preceptos que regulan la responsabilidad patrimonial de la administración pública (p. 197).

Es entonces que surge la pregunta: ¿Es responsabilidad del estado tener seguridad jurídica en el envío y recepción de documentos electrónicos?

> Con este trabajo de investigación, se pretende recopilar información de fuentes confiables que indiquen la existencia de un sistema de seguridad jurídico para el uso de documentos electrónicos, así mismo, servirá como apoyo para obtener conocimiento acerca del tema teniendo en cuenta las conceptualizaciones relevantes y conocer acerca del marco legal que existe en Colombia con respecto al tema, el sistema ha de garantizar las propiedades de autenticación de origen y destino e integridad de los documentos remitidos entre jueces, secretarios y procuradores mediante la utilización por todos ellos de recursos criptográficos, especialmente la firma electrónica, también se garantizará la confiabilidad de los mensajes (Huerta Miranda & Líbano Manzur, 2008, p. 1).

Es importante mencionar que mediante el derecho se deben encontrar soluciones para el uso desmedido del mundo virtual. Becerra (2002) afirma:

> El reto consiste, entonces, en flexibilizar las instituciones jurídicas e incorporar aquellos usos reiterados, públicos y uniformes que han surgido en Internet, para que

> las consecuencias jurídicas sean las mismas tanto en los negocios jurídicos que se realizan en el mundo real o físico, como en los que se celebren en el mundo virtual (p. 80).

1. Problema jurídico

El problema de investigación al que contribuye esta monografía es el siguiente: ¿Existen actualmente herramientas para proveer de protección jurídica a los documentos electrónicos? es de tener en cuenta que este tema de investigación es extenso donde varias conceptualizaciones se unen entre sí para dar respuesta a la problemática.

2. Tesis

En la actualidad la seguridad de los documentos electrónicos es de gran relevancia para el mundo entero como para el país, es necesario determinar si existen las herramientas suficientes para dar seguridad a los documentos que son realizados y almacenados de forma electrónica, así mismo, dar la confianza al ciudadano de que dicha documentación es verídica. En el presente trabajo se busca explicar acerca de las herramientas utilizadas para dar seguridad y garantizar la integridad de la información enviada y recibida electrónicamente. A pesar de que en nuestro país se ha orientado acerca del adecuado uso de la información en las nuevas tecnologías para evitar el uso ilegal de la información, aún queda mucho por hacer con el fin de garantizar confidencialidad y autenticidad de los documentos electrónicos.

3. Objetivos

3.1. Objetivo general

Determinar las herramientas actuales para dotar de seguridad jurídica a los documentos electrónicos.

3.2. Objetivos específicos

- Identificar los factores que perjudican la seguridad jurídica de los documentos electrónicos.
- Investigar las posibles soluciones para mitigar la presencia de factores que perjudican la seguridad jurídica de los documentos electrónicos.
- Analizar el estado de seguridad jurídica de documentos electrónicos en Colombia.

4. Metodología

La metodología empleada en este trabajo fue basada en la investigación previa de sucesos, características y estadísticas de acuerdo al tema antes mencionado. La recolección de información se realizó mediante la lectura de fuentes bibliográficas referentes a la problemática expuesta, trayendo como resultados la identificación de los factores que perjudican la seguridad de los documentos, así mismo se encontró información relevante para interpretar las posibles soluciones a estos factores y por último, permitió llevar a cabo el análisis de la situación actual del país en el tema.

5. Antecedentes de investigación

Para el Dr. Marco Emilio Sánchez y sus colaboradores en el libro *La responsabilidad del Estado por la utilización de Tecnologías de la información y la comunicación*. Indican que el Internet ha pasado a ser esencial para la vida. Becerra (2015) afirma:

> Es un instrumento indispensable para ejercer libertades (expresión, información, asociación) y derechos participativos y sociales (educación, cultura, etc.), el cual se ha considerado como un vehículo para mejorar la igualdad de oportunidades y la generalización de servicios de los poderes públicos que antes eran casi inimaginables. Es por ello que está emergiendo la consideración de que el acceso a Internet es un derecho fundamental autónomo de última generación (p. 197).

Así mismo indican Becerra, García, Sánchez & Torres (2015):

> Como nuevo derecho tendría un componente prestacional muy importante, que conlleva como corolario toda una serie de obligaciones de actividad del Estado. Pero también sería un viejo derecho esencialmente negativo, en la órbita de la libertad de expresión e información, que garantiza que el Estado no ponga barreras o censure el acceso mismo a la red y a sus contenidos (p. 197).

De acuerdo con Becerra (2015)

> En cuanto a la publicación de contenidos por parte de la administración y su marco de responsabilidad, es necesario determinar el cumplimiento o cumplimiento defectuoso de los principios y requerimientos legales de seguridad de la información, así como de los controles de seguridad impuestos en el nivel reglamentario (p. 198).

Con estas afirmaciones se puede observar que el tema de seguridad de la información electrónica también compete y debe ser estudiado por el estado, con el fin de prestar a usuarios de redes electrónicas seguridad en la exposición de documentos en la nube.

Por otro lado, Velasco (2008),

> busca informar sobre la existencia y diversas modalidades que incluye el Derecho informático y crear conciencia acerca de la posición que deben tomar los diversos actores económicos en la era de la información para asegurar una adecuada política de seguridad de la información que, ante la falta de una legislación nacional sobre el tema, debe basarse en los estándares internacionales, el derecho comparado y autonomía de la voluntad (p. 334).

Velasco (2008) afirma:

> La seguridad informática ha hecho tránsito de un esquema caracterizado por la implantación de herramientas de software, que neutralicen el acceso ilegal y los ataques a los sistemas de información, hacia un modelo de gestión de la seguridad de la información en el que prima lo dinámico sobre lo estacional. Para lograr niveles adecuados de seguridad se requiere el concurso e interacción de las disciplinas que tengan un impacto en el logro de este cometido, teniendo siempre presente que un sistema de gestión no garantiza la desaparición de los riesgos que se ciernen con mayor intensidad sobre la información. Entonces, el problema es determinar cómo desde una disciplina como el Derecho se contribuye a la gestión de la seguridad de la información. Los enfoques de intervención jurídica podrían ser muchos; de hecho, no existe limitación alguna, para que una organización adopte las medidas que considere pertinentes con el fin de neutralizar un riesgo (p. 339).

Como afirma Díaz García (2010)

> Desde la perspectiva del derecho o la ciencia jurídica, más concretamente del derecho informático y frente al tema de las redes telemáticas y el intercambio electrónico de datos, documentos estandarizados y valores, existen diversas cuestiones jurídicas de relevancia que deben ser analizadas, como: la firma electrónica o digital como sustituto de la tradicional firma escrita, la seguridad y la privacidad de las transmisiones (teniendo en cuenta si son de naturaleza especial), naturaleza jurídica y valor probatorio de los documentos transmitidos electrónicamente, domicilio virtual y otros factores son necesarios determinar al momento de realizar transacciones de documento electrónicos (p. 2).

Por otro lado, Rendón López (2009).

> Actualmente existen nuevas y novedosas oportunidades para el intercambio de información a través de las tecnologías de la información y comunicación, correlativo a ello, también han surgido nuevos riesgos a la seguridad de la misma y, en consecuencia, se han creado mecanismos que garanticen la confidencialidad y autenticidad de la información y los documentos electrónicos que la contienen y se utilizan para transmitirla. Por lo tanto, en su trabajo intenta exponer de manera

> general la problemática real que aqueja a los documentos electrónicos en su camino por el ciberespacio, sobre todo en lo referente a su confidencialidad y autenticidad, así como la forma en que la criptografía ha mitigado sus efectos (p. 1). Siendo esta una herramienta fundamental para la mitigación de la problemática existente.

Desde la posición de Díaz Miranda (2006) en su tesis de grado en el cual hace una recomendación donde indica que

> Los notarios de fe pública deben concentrarse en su actividad de asesorar, interpretar la voluntad, de dar forma, de legalizar, legitimar y sobre todo de dar fe pública en la creación de documentos electrónicos auténticos. El papel de los notarios electrónicos es clave para la seguridad jurídica de los documentos electrónicos, por lo que debe ya instalarse, mediante Ley expresa, los notarios electrónicos (p. 178), es decir, hace recomendación a la creación de notarios electrónicos que sean expertos en el área.

Díaz (2006) afirma:

> La certificación de firma electrónica, a través de una autoridad certificante por su importancia en el avance de la tecnología, debe ser obligatoria y de carácter general para todos, siendo así, permitiría identificar inequívocamente al firmante del documento electrónico, evitando la posibilidad del posterior repudio o alternativamente de fraude o daños patrimoniales (p. 178).

En Colombia contamos con una ley, denominada Ley 527 de (1999), en el cual se "define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones" (p. 1). La realización, traspaso, almacenamiento u otra actividad de documentos electrónicos, se ve amparada mediante esta Ley de la República, uno de los beneficios de la ley se basa en el caso de plagio de acuerdo al origen del documento es decir sea un documento en físico original o redactado de manera virtual, se puede verificar como sucedió el incidente informático, así mismo, "hay aplicaciones como evLab que permite que se cumpla con los requisitos de la Ley 527 de 1999 que, en su artículo 6, 7 y 8" establece que, "cualquier documento es reconocido, sin importar su formato, como un

documento electrónico, sin embargo, es necesario tener metodologías para identificar su veracidad, proceso que se hace más fácil con los documentos que nunca fueron análogos" (p. 2).

En ese mismo orden señala el Artículo 209 "La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones" (Constitución Política de Colombia, 2020, Art. 209). Es ese el mandato del Artículo 1 de la Ley 1437 de 2011, cuando indica que la finalidad de dichas normas es:

> […] proteger y garantizar los derechos y libertades de las personas, la primacía de los intereses generales, la sujeción de las autoridades a la Constitución y demás preceptos del ordenamiento jurídico, el cumplimiento de los fines estatales, el funcionamiento eficiente y democrático de la administración, y la observancia de los deberes del Estado y de los particulares (Congreso de Colombia, 2011, p. 1).

El servicio o cargo administrativo, nos brinda la oportunidad y la seguridad, de acceder a un servicio, ético, profesional; apto del público en general, y basado además en nuestras raíces culturales, y estado actual gubernamental. Para los clientes a nivel nacional e internacional es necesario conocer las condiciones, y la reglamentación mediante como cuerpo empresarial ofrecemos una garantía de calidad hacienda nuestros clientes. Jiménez y Meneses (2017) afirman:

> Paralelamente se dio origen al correo electrónico, en la actualidad uno de los servicios más populares de Internet; pues fue en 1965 cuando se usó el primer sistema de correo electrónico llamado mail box en el Massachusetts Institute of Technology. Antes que Internet se desarrollara, los correos electrónicos solo podían ser enviados por usuarios de un mismo computador (usualmente alrededor de cien personas), conectados desde sus escritorios mediante dumb terminals (terminales mudos), los cuales no tenían capacidad de almacenamiento ni memoria (p. 46).

La tecnología ha sido de vital importancia para superar las distintas barreras comerciales, que se pueden presentar en el mercado; el uso del correo electrónico, el acceso a las distintas redes ha colocado a otro nivel, todo lo que pensamos que ya no podía mejorar, o que no podría revolucionar el mundo, en unos años más tarde se encuentra siendo la herramienta virtual, formal y más rápida de todo el mercado.

De acuerdo con Pequera Poch (2005)

> Internet se basa en una arquitectura cliente-servidor, ya que la mayoría de las aplicaciones y servicios que se pueden encontrar siguen este modelo. La parte servidor espera permanentemente a recibir peticiones del cliente. Cuando el cliente genera una petición, el servidor sirve la información o servicio que el cliente ha solicitado (p. 25).

La internet, nos ha mostrado una amplia gama de posibilidades; le brinda al mundo entero la posibilidad de vender, intercambiar, negociar, reformar, y mejorar nuestro estado económico, el uso que le amos a esta herramienta, debería trabajar en PRO del crecimiento humano, donde ningún ciudadano, ningún núcleo familiar se encuentre en desventaja. Torres (2015) afirma:

> El cambio tecnológico parece escapar de las posibilidades de esta fundamentación, pues una de sus características es, justamente, la enorme velocidad a la cual no solo se presenta como objeto de la invención, sino que, en realidad, presenta un fuerte impacto en el campo de la innovación; es decir, en la transformación de hábitos y usos de la tecnología en la vida de las personas. Incluso, podríamos decir que es una característica de las sociedades contemporáneas basar parte de su funcionamiento y de su desarrollo en la perspectiva del continuo cambio tecnológico (p. 55).

Sin duda alguna los avances científicos también se basan en los avances tecnológicos, que han apoyado, la investigación y la documentación de gran importancia para el desarrollo y la perduración de la especie humana; cada núcleo social, trae con ella una

cultura, un pensamiento, unas raíces, una historia completamente diferente, sin importar la consanguinidad de cada uno de ellos, y ese es el punto principal, reconocer, que a pesar de las conexiones o relaciones interpersonal, cada grupo social tiene un pensamiento, un criterio, una verdad.

Dicho con palabras de Alvite Díez (2009)

> La formalización de las ontologías se asienta en el lenguaje propio de la Web semántica (OWL-Web Ontology Language), un lenguaje que emplea RDF/XML para representar y codificar ontologías. En el ámbito del Derecho, como apuntan Vallbé et al. (2007), el área jurídica se ha mostrado especialmente interesada en el desarrollo de ontologías que propicien la implementación de aplicaciones "más inteligentes". Los mismos autores subrayan dos diferencias claves en las ontologías jurídicas frente a otras ontologías (p. 41).

El lenguaje y todas sus variaciones, nos ayudan a establecer, planos para ejecutar las distintas labores, o tareas con los que nos podamos desarrollar o adaptar; lograr avances inteligentes que puedan redefinir nuestra capacidad de pensamiento y comunicación.

6. Marco teórico

6.1. Concepto de documento electrónico

Iniciemos con la conceptualización documento; Becerra (2002) afirma

> En el sentido etimológico, documento proviene del vocablo latino documentum, que significa aquello que enseña o aquello con lo que alguien se instruye. También se acepta que la expresión en griego dékomai como origen de la expresión documento el cual significa "Yo hago a alguien algo claro o yo enseño (p. 3).

El profesor Colombiano Medina Torres (2001), "expone que el documento es una cosa que enseña" (p. 32). Por otro lado, el profesor Rengifo García (2000) "expone que un documento es cualquier objeto que contiene una información, que narra, que hace conocer

o que representa un hecho, cualquiera que sea su naturaleza, su proceso de elaboración y su tipo de forma" (p. 3).

> El Código de Procedimiento Civil Colombiano, en su artículo 251 establece que, en general, documento es todo objeto mueble que tenga carácter representativo o declarativo, y a manera de ejemplo, sólo por ilustrar, la norma en cita pregona que son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas y sellos. (Becerra, 2002, p. 3).

Al hablar de documento electrónico posiblemente exista la confusión entre un documento informático y el documento electrónico, el primero comprende todo tipo de documentación que sea guardada ya sea en el CPU o algún disco duro, tal como; trabajos, mensajes, documentos, contratos, informes entre otros.

Teniendo en cuenta a Rendón López (2009),

> los documentos electrónicos aquéllos que no solo reproducen, sino también materializan una cierta manifestación de voluntad para ser percibidos y comprendidos por el hombre, a través de las tecnologías de comunicación e información, mediante mensajes digitalizados y sistemas inteligentes o expertos (p. 6).

Actualmente nos preguntamos qué sucede con el ciclo de vida de los documentos. Continuando con la definición de documento electrónico; "en el panorama de los documentos electrónicos, se vuelve cada vez más evidente que el ciclo de vida de los documentos debe ser el nuevo foco de atención". Redondo Herranz (2010) afirma:

> La terminología usada por los especialistas en documentos electrónicos es muy diferente de la terminología diplomática, pero el mensaje transmitido es claro: la comprensión de los procedimientos es la clave para la comprensión de los sistemas de información en los que están incluidos estos documentos electrónicos. Por esa razón, los documentos deben ser clasificados de acuerdo a las funciones y actividades de sus creadores mediante la reconstrucción y examen de los

> procedimientos de la creación documental, porque cada vez existe una mayor necesidad de entender las rutinas que rigen la creación de los documentos (p. 392).

Dicho de otra manera, el conocimiento de la génesis documental es la clave para comprender la "forma" y el "discurso" diplomáticos y es que el documento electrónico, curiosamente, busca en sus nuevas formalidades las mismas antiguas características de autenticidad, fiabilidad, integridad y permanencia del tradicional documento escrito, ya que sigue siendo como en otras épocas un instrumento de constancia, más o menos permanente, de actos y hechos de la gestión administrativa (p. 2).

6.2. Requisitos del documento electrónico

Para que un documento electrónico sea válido y confiable debe cumplir con ciertos requisitos estandarizados que traerán beneficios en materia de información.

Dicho con palabras de Redondo (2010)

> Es importante que un documento sea autentico, es decir, que la información contenida sea totalmente cierta, sin importar cuál sea su rama informativa. Hasta ahora esa garantía venía dada por la firma del autor del documento, sin embargo, en los nuevos documentos electrónicos tendrá que configurarse con una serie de elementos de seguridad determinados, en lo que se conoce como firma electrónica reconocida, más adelante se mencionara información relevante acerca de la firma electrónica para mayor entendimiento (p. 397).

> Para garantizar que el documento electrónico no haya sufrido alteraciones, es importante asegurar la Integridad, en las informaciones en él contenidas durante la transmisión entre distintos sistemas una vez el documento electrónico haya sido autenticado mediante la firma electrónica del autor (Redondo, 2010, p. 397).

Redondo (2010) afirma “Estos sistemas pueden ser tanto sistemas de la misma organización donde se ha generado el documento, como redes públicas o privadas de comunicación con terceras personas (física o jurídica)” (p. 397).

Otro requisito fundamental es la Originalidad la cual que viene determinada por la génesis del documento dentro de un contexto determinado de producción.

> “Sin embargo, un original electrónico no tiene por qué mantener la estructura de disposición de la información desde el momento de su génesis hasta el de su comunicación en contra de lo que viene sucediendo con los documentos en papel” (Redondo, 2010, p. 397).

Redondo (2010) afirma

> El documento electrónico no tiene por qué ser conservado en el mismo programa informático en que fue producido, su forma de presentación podría variar según los criterios de gestión y conservación que se establezcan en los sistemas de archivos, y es que una vez finalizada la tramitación administrativa y transferido el archivo se pueden definir formatos de conservación diferentes al formato de creación (p. 397).

> “Por último, la seguridad vendrá determinada por la política de seguridad de acceso a los sistemas de producción administrativa de la organización donde se generen los documentos electrónicos, y por la firma electrónica como garantía de identificación fehaciente de la autenticidad del firmante, y de la integridad de la información registrada en el soporte electrónico” (Díaz, 2002, p. 69).

Redondo (2010) afirma: “Así mismo la autenticidad e integridad serán dos elementos que manifiesten la originalidad de estos documentos” (p. 397).

> Una cosa es que un documento exista, permanezca en buen estado, y otra cosa es que se pueda acceder y se pueda ver y analizar su contenido. Habrá o no

> "accesibilidad", independientemente de su "permanencia". Esta es la acepción de usabilidad que deberá usarse en lo relativo a preservación y seguridad. No debe confundirse este término con el concepto de "accesibilidad" como "usabilidad" en el sentido de las facilidades que se les agregan a ciertos sitios Web para que puedan ser accedidos más fácilmente por personas con capacidades visuales diferentes, tales como fuentes de letras más grandes, contrastes de colores más pronunciados, "lentes de aumento" virtuales sobre la pantalla, etcétera (Voutssas, 2010, p. 135).

6.3. Seguridad jurídica

Como expresa Sánchez (2003) “la seguridad jurídica la define como el conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados” (p. 39). Maza Márquez (1998) afirma “Así como no hay códigos inviolables tampoco hay redes totalmente seguras. Aparecen defectos y fallas, no puede preverse todo lo que va a suceder. Pero es mejor tenerlo todo en cuenta” (p. 245). Los daños producidos se basan en un mal funcionamiento del hardware, perdida de datos o el ingreso a sistemas confidenciales de personas no autorizadas, así como otros factores que se mencionaran próximamente.

Si entramos en materia de seguridad, Jovel Sánchez (2003) afirma “existen técnicas sencillas que dificultan la delincuencia informática tales como destruir la información impresa, impedir que otros observen la pantalla, mantener la información y los equipos bajo llave o cuidando la información valiosa, pueden ser las soluciones más sencillas” (p. 40); sin embargo cuando hablamos de delitos informáticos se requieren sistemas más complejos, porque por los avances de la tecnología, cualquier información privilegiada puede verse afectada por sistemas dañinos o hackers de información.

Como expresa Voutssas (2010) en su artículo de investigación los objetivos a los cuales se rige la seguridad jurídica de los documentos electrónicos, como principio básico menciona que la seguridad informática no es un producto, es un proceso. Así mismo menciona que,

> […] el objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable (Barnard, Delgado & Voutssás, 2014, p. 22).

El segundo objetivo se basa

> […] en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total. Este concepto varía de acuerdo a distintos autores, a los contextos documentales y al tipo de organización a la que la información esté asociada (p. 132).

6.4. Factores que perjudican la seguridad informática

"La seguridad informática se ve afectada por muchas situaciones o particularidades, sobretodo en el mundo virtual, ya que por medio del uso del internet o estudios informáticos se puede lograr el robo de información de los documentos electrónicos" (Seguridad informática, p. 1).

6.4.1 Tecnológicos.

"Son fallos a nivel de hardware y/o software. La mayor amenaza proviene de software malicioso: virus, malware, etc. Estos son programas con un alto poder de infección y que se auto replican para aumentar su difusión" (Seguridad informática, p. 1).

6.4.2. Humanos.

> Hackers y Crackers suponen una amenaza a la seguridad informática de equipos y redes. Los primeros por su interés en probar si un sistema tiene fallos reportándolo después al resto de la comunidad. Los crackers por su parte buscan acceder a los sistemas para robar o destruir información a veces aprovechando las vulnerabilidades descubiertas por los hackers y en otras aprovechando la infección de programas maliciosos que les permiten acceder con total libertad a ordenador infectado (Seguridad informática, p. 1).

6.4.3. Ambientales.

> Los factores ambientales son impredecibles. Fenómenos naturales de grandes proporciones pueden afectar al funcionamiento de máquinas y equipos informáticos si quedan afectadas infraestructuras básicas que les suministren energía. Lluvias torrenciales, tormentas eléctricas, calor excesivo forman parte de esos factores ambientales a valorar (Seguridad informática, p. 1).

6.5. Parámetros de seguridad informática

Tras efectuar un ejercicio de análisis de riesgos informáticos valorando todos los activos físicos y digitales que se dispongan habrá que proceder a:

1. Comunicar a todo el personal involucrado del desarrollo de las políticas de seguridad informática que vayan a establecerse.
2. Identificar a las personas o entidades que tengan autoridad para tomar decisiones ante riesgos de seguridad informática establecidos o no en las políticas diseñadas.
3. Monitorear de forma periódica el cumplimiento de las directrices marcadas según lo establecido en el documento de políticas de seguridad en los sistemas y equipos informáticos (Seguridad informática, p. 1).

6.6. Amenazas

Una amenaza consiste “en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma” (Voutssas, 2010, p. 2).

> La llegada y proliferación de "malware" o "malicious software" los cuales son programas cuyo objetivo es infiltrase en los sistemas sin conocimiento de su dueño, con el fin de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización. Por otro lado, otra amenaza se basa en la pérdida, destrucción,

> alteración, o sustracción de información por parte de personal de la organización debido a negligencia, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas (Voutssas 2010, p. 2).

"Así mismo, la pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados, así como también, el acceso no autorizado a conjuntos de información" (Zambrano, 2017).

Granger (2009) afirma

> Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de cibercriminales lo cuales son personas o grupos malintencionados que apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión. Por otro lado, Los llamados "phishers", quienes son especializados en el robo de identidades personales y otros ataques del tipo de "ingeniería social (p. 139).

Los "spammers" y otros mercadotecnitas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.

Y, por último, es importante mencionar también, Quiroz Zambrano y Macías Valencia (2017) "la pérdida o destrucción de información debido a accidentes y fallas del equipo, es decir, fallas de energía, fallas debidas a calentamiento, aterrizamiento, desmagnetización, rayadura o descompostura de dispositivos de almacenamiento u otros" (p. 683). Otros percances físicos como;

> pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera y la aparición de tecnologías avanzadas tales como el cómputo quamtun, mismas que pueden ser utilizadas para desencriptar documentos, llaves, etcétera al combinar complejos principios físicos, matemáticos y computacionales (Voutssas, 2010, p. 3).

6.7. Vulnerabilidades informáticas

> Cuando se habla de vulnerabilidad hablamos de una característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza intencional o accidentalmente. Las vulnerabilidades informáticas pueden provenir de muchas fuentes, desde el diseño o implementación de los sistemas, procedimientos de seguridad, controles (Granger, 2009, p. 1)

De seguridad u otros, es decir, se trata de protecciones inadecuadas o insuficientes en el ámbito físico y lógico.

Con respecto a aspectos humanos también pueden existir inconvenientes que afecten la seguridad informática como;

> la confianza excesiva en algún único dispositivo u oficina de seguridad, desacato o relajamiento de las políticas y procedimientos de seguridad, debidos a falta de seguimiento de los mismos, producidas por un desempeño de seguridad adecuado durante cierto lapso, existencia de fallas de seguimiento en el monitoreo o indicadores de seguridad, pobre o nula gobernanza de los activos informáticos, debida principalmente a un mal seguimiento de esos activos y sus contextos de seguridad asociados de forma integral, cambio frecuente de elementos de la plataforma informática, falla en la adjudicación o seguimiento de responsabilidades, planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas, la ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas (Voutssas, 2010, p. 1),

También es un caso que puede inducir a errores que pueden afectar la seguridad y tener en cuenta “la falta de concientización del personal en general acerca de la importancia de la seguridad y responsabilidades compartidas e integrales” (Granger, 2009, p. 1).

6.8. Riesgos informáticos

Riesgo es definido “como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Y este se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto” (Granger, 2009, p. 1).

> Sustracción de datos personales para usos malintencionados. Fugas de información, extracción o pérdida de información valiosa y/o privada. Introducción de programas maliciosos a los sistemas de la organización, que pueden ser utilizados para destruirlos u obstaculizarlos, usurpar recursos informáticos, extraer o alterar información sin autorización, ejecutar acciones ocultas, borrar actividades, robo y detentación de identidades, etcétera. Acciones de "ingeniería social" malintencionada: "phishing", "spam", espionaje, etcétera. Uso indebido de materiales sujetos a derechos de propiedad intelectual. Daño físico a instalaciones, equipos, programas, etcétera (Granger, 2009, p. 1).

6.9. Impactos

Los factores mencionados anteriormente producen impactos negativos los cuales son definidos “como efectos nocivos contra la información de la organización al materializarse una amenaza informática” (Granger, 2009, p. 1).

> Disrupción en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa, se puede incitar a la pérdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, del público en general y hasta de los medios de información (Granger, 2009, p. 1).

De acuerdo a todo lo mencionado anteriormente el proceso de seguridad informática busca identificar las amenazas y reducir los riesgos mediante la mitigación o eliminación de estos problemas tecnológicos y de cuidado humano en ciertos casos, para concluir se indica que la seguridad informática se define como

> […] el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos (Voutssas, 2010, p. 1).

6.10. Criptografía como solución a la inseguridad jurídica de documentos electrónicos

Según Jovel Sánchez (2003) en su trabajo de investigación *El Documento Electrónico, la Firma Digital y la Contratación* define "la criptografía como la ciencia que trata el enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente" (p. 41). Jovel (2003) afirma:

> Es decir, abarca el uso de mensajes encubiertos, códigos y cifras, estos mediante la utilización de mensajes ocultos escritos con tinta invisible, la idea fundamental es no levantar ninguna sospecha. En mucho sentido, "la palabra se limita a la utilización de cifras, es decir, métodos de transponer las letras de mensajes (no cifrados) normales o métodos que implican la sustitución de otras letras o símbolos por las letras originales del mensaje, así como a diferentes combinaciones de tales métodos, todos ellos conforme a sistemas predeterminados" (p. 41).

Por otro lado, otra definición es la mencionada por Villalobos (1990), quien indica que "es la ciencia que estudia la ocultación, disimulación o cifrado de la informática, así como el diseño de sistemas que realicen dichas funciones" (p. 88). Sea cual sea el autor, llegan a la conclusión que la función principal de la criptografía es ocultar la información mediante una serie de códigos que solo puedan ser cifrados por profesionales o personal autorizado.

“En las claves de transposición, el mensaje se escribe, sin separación entre palabras, en filas de letras dispuestas en forma de bloque rectangular” (Ontaneda, 2009). Jovel (2003) afirma:

> Las letras se van transponiendo según un orden acordado de antemano, por ejemplo, por columnas verticales, diagonales o espirales, o mediante sistemas más complicados, como el salto el caballo, basado en el movimiento del caballo de ajedrez. Para aumentar la seguridad de la clave o cifra se puede utilizar una palabra o un número clave; por ejemplo, a la hora de transponer por columnas verticales, la palabra clave coma obligaría a tomar las columnas en el orden 2-4-3-1, que es el orden alfabético de las letras de la palabra clave, en lugar de la secuencia normal 1-2-3-4. Con tiempo y medios suficientes se pueden descifrar la mayoría de las claves, pero en cada caso se deberá utilizar el grado de complejidad suficiente para alcanzar el nivel de seguridad deseado (p. 42).

Como señala Rendón López (2009)

> la criptografía se configura mediante una serie algoritmos, los cuales consta realizan la función de codificar la información para que sea indescifrable a simple vista, de manera que una letra "A" pueda equivaler a: "2x4AeaA", por ejemplo; es entonces que el algoritmo determina cómo será transformada la información de su estado original a otro que sea muy difícil de descifrar (p. 10).

6.11. Tipos de cifrado

6.11.1. Simétrico.

> Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son muchos más rápidos que los de clave pública y resultan apropiados para el cifrado de grandes volúmenes de datos (Echeverría, 2013, p.138).

> Para ello se emplean algoritmos (estructuras lógicas que denotan una instrucción u orden) como IDEA (International Data Encription Algorithm), RC5, DES (Data Encription Standart), TRIPLE, PGP (Pretty Good Privacity), etc (Echeverría, 2013, p. 138).

Hoy por hoy, los ordenadores pueden adivinar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos" (GNU Privacy Guard, 2012). Para entender un poco más esta guía emplea un ejemplo;

> el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 256 claves posibles. 256 son 72.057.594.037.927.936 claves, esto representa un número muy alto de claves, pero una máquina computadora de uso general puede comprobar todo el espacio posible de claves en cuestión de días (GNU Privacy Guard, 2012).

6.11.2. Asimétrico.

> Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos, es decir, las claves públicas se utilizan para cifrar y las privadas para descifrar (López, 2009, p. 11).

Rendón López (2009) afirma

> El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada, ni descifrar el texto con ella cifrado. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales (p. 12).

Este tipo de cifrado suele usarse comúnmente en claves de sesión para información y documentos públicos, ya que permite la transmisión de la información sin peligro a través de la red junto con el documento cifrado. Rendón López (2009) afirma “La clave de sesión se cifra como pública y normalmente aparecerá en una libreta de claves públicas. Un ejemplo de ello es el One Time Password (contraseña de un solo uso) o clave de sesión” (p. 12).

“Los sistemas de cifrado de clave pública se basan en funciones trampa de un sólo sentido. Una función de un sólo sentido es aquélla cuya computación es fácil, mientras que invertir la función es extremadamente difícil” (GNU Privacy Guard, 2012).

6.12. PGP (Pretty Good Privacity) como Criptografía de Alta Seguridad

Según Pontiroli (2013), líder mundial en seguridad, donde redactan una breve reseña de

> PGP – Privacidad, seguridad y autenticación fiables para todos, es un programa creado por Phil Zimmermann que nos ayuda a proteger nuestra privacidad, para que todas las comunicaciones estén a buen seguro; al mismo tiempo, garantiza la autenticidad de los mensajes electrónicos que enviamos (p. 1).

Según Zimmermann (2019);

> diseñó PGP hace más de 20 años y desde entonces se han realizado muchas mejoras. Al principio, el gobierno estadounidense investigó a Zimmermann “por exportación de municiones sin licencia”, ya que los productos de encriptación más fuertes de 40 bits (PGP era un producto de 128 bit) se consideraban como municiones. Aunque se cerró el caso sin cargos para Zimmermann, se demostró cómo de potente puede ser una herramienta de encriptación y por qué algunos importantes accionistas de empresas tienen tanto interés en este asunto (p. 1).

Este blog creado por Kaspersky Daily trae más información de cómo usar el PGP como sistema de seguridad para los documentos electrónicos, indica los conceptos básicos del programa, dan recomendaciones y explican cómo es usado de una manera fácil. Pontiroli (2013) afirma

> Con la llegada de PGP, las cosas cambiaron. Al principio el usuario común no sabía cómo mantener seguras sus comunicaciones e su información personal, ni tampoco empresas y otras entidades querían que se encontrara un método. Por suerte, después de 20 años, PGP ha colmado este vacío, demostrando ser un sistema capaz de garantizar privacidad y libertad (p. 10).

6.13. La firma electrónica y firma digital o llaves

El literal C del artículo 2º. De la ley 527 de 1999, en Colombia, define la firma digital como

> un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación (Firma digital, 2019).

Por otro lado, podemos encontrar otras definiciones donde se explica a detalle lo que a una firma electrónica se refiere; El doctor Henao Restrepo (2000) en su participación en el XV Congreso Nacional de derecho comercial, Medellín 1999, *Nuevos retos de derecho comercial* afirma

> La firma digital es un instrumento que garantiza tanto la autenticidad de un documento como la integridad del mismo. Estos caracteres son puestos en el documento por su creador mediante una llave privada que sólo él conoce, previamente asignada por una entidad certificadora (p. 88).

Así mismo, el doctor Rengifo García (2000) en colaboración y participación en el mismo congreso, afirma

> la firma digital consiste en la transformación de un mensaje empleando un criptosistema asimétrico tal que, una persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante y si el mensaje ha sido modificado desde que se efectuó la transformación. Un criptosistema asimétrico es un algoritmo o serie de algoritmos que brindan un par de claves confiables (clave pública y clave privada), (p. 88).

Ahora bien, en tema de seguridad, Jovel (2003) afirma:

> […] la firma digital proporciona seguridad adicional y le permite al receptor del mensaje, verificar su procedencia y su contenido, pero hay que tener presente que ella por sí sola no representa garantía de confidencialidad, este campo le compete a la criptografía, para asegurar un documento de manera confiable es importante que ambas técnicas sean empleadas al unísono (p. 22).
>
> Para entender un poco más de su funcionamiento el Licenciado Jovel Sánchez (2003) afirma "la firma digital emplea dos llaves criptográficas para cada usuario, una pública que es conocida por todos los clientes potenciales y otra privada que debe mantenerse en secreto. El receptor obtendrá un mensaje y la firma digital" (p. 42).
>
> Un algoritmo de verificación de firma es usado por él para autenticar al firmante de la transacción, este algoritmo usa la información de la clave pública del remitente, el contenido del mensaje y la firma digital para realizar los cálculos, si el resultado es correcto el remitente es autenticado y por ende el mensaje recibido es idéntico a

> aquel enviado, si la verificación de la firma falla la transacción es rechazada y se solicita una retransmisión (p. 22).

Como expresa Jovel (2003)

> existen muchos algoritmos de firma digital descritos en la literatura, pero en la práctica se usan principalmente tres: la firma fragmentada, la firma digital del gobierno de los Estados Unidos de Norteamérica (Digital Signature Standard: DSS) y el sistema RSA creado usando los algoritmos clásicos, el cual fue desarrollado por Ron Rivest, Adi Shamir y Len Adleman, cada uno de ellos tiene un uso distinto (p. 44).

Jovel (2003) afirma:

> La firma fragmentada es un sistema de encriptación ligeramente modificado que puede usar los protocolos MID-5 (Message Digest 5) o el Algoritmo de
>
> Fragmentación Segura SHA (Secure Hash Algorithm), para producir un resultado fragmentado partiendo de un archivo. El procedimiento de fragmentación conecta su clave secreta con el archivo (la cual tiene que haber sido proveída por un tercero) el resultado es un valor fragmentado que es exportado con el documento a manera de firma, la cual será verificada por el receptor quien también tiene la clave secreta y es este aspecto su mayor limitación porque él podría falsificar un mensaje en nuestro nombre, además de que es molesto guardarla (p. 45).

“El sistema DSS funciona con la clave pública (verifica la firma) y la privada (crea la firma) fue creado por el gobierno de E.U.A., pero su uso no es muy difundido” (Firma electrónica, 2000). Jovel (2003) afirma:

> El sistema RSA es el más popular en parte por su mercadeo, sistema de patente y desarrollo a largo término. La compañía que lo implementó controla muchas de las patentes en este campo, por lo que es líder y emplea a los mejores criptógrafos (p. 45).

Como plantea Jovel (2003)

> los sistemas de clave pública son los más fáciles de atacar, sobre todo por el hecho de que las dos partes conocen la clave y además son fácilmente sustraíbles, existe una forma de hacerlos más seguros y es envolviendo la firma en un certificado de autenticidad, que es un pequeño bloque de datos (tal vez de algunos miles de bytes de largo) que contendrá la llave pública y el endoso hecho por la firma digital de alguien más, éste será la Autoridad Certificadora, que puede ser una empresa como Veri Sign. En el campo de los certificados pueden obtenerse varios tipos, por ejemplo, considerando el caso concreto de Veri Sign, el certificado tipo 1 es el que obtiene cualquiera que pueda llenar un formulario en la red, el tipo 2 es expedido luego de que son verificados algunas bases de datos sobre el cliente (p. 45).

Jovel (2003) afirma "El certificado clase 3 requiere que el cliente se presente ante un notario y ante él o ella confeccione la solicitud, así luego el funcionario la endosará, agregando una capa adicional de credibilidad al certificado" (p. 45).

Por otro lado, entrando en materia jurídica, Morales Sánchez (2016) afirma "en su trabajo de investigación realiza una recopilación de las normas colombianas que se vinculan al tema de la firma digital" (p. 41).

"Decreto No. 1165 de 15 de Julio de 1996. Reglamenta varios artículos del Estatuto Tributario y reconoce la equivalencia de la factura electrónica (Artículo 5to) como documento equivalente a la factura de venta" (Morales, 2016, p. 41).

"Ley No. 527 de 18 de agosto de 1999. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y establece las Autoridades de Certificación" (Morales, 2016, p. 41).

"Decreto No. 1.747 de 11 de septiembre de 2000. Reglamenta parcialmente la Ley No. 527, en lo relacionado con las Autoridades de Certificación, los certificados y las firmas digitales" (Morales, 2016, p. 41).

“Resolución No. 26.930 de 26 de octubre de 2000” (Morales, 2016, p. 41).

“Decreto No. 4149 de diciembre 10 de 2004. Crea la ventanilla Única de Comercio Exterior” (Morales, 2016, p. 41).

“Ley 962 (Ley Antitramites) de 8 de Julio de 2005. Se racionalizan los trámites y procedimientos administrativos. Decreto No. 1929 de 2007 se establece la posibilidad de facturar electrónicamente” (Morales, 2016, p. 41).

Citando a Rincón (2008) “Ley 794 de 20043, que establece la posibilidad de desarrollar actos de comunicación procesal por medios electrónicos, utilizado firma digital” (pp. 102-103).

7. Seguridad jurídica de documentos electrónicos en Colombia (marco legal)

Aunque no se crea que los usos de nuevas tecnologías han afectado de manera positiva y negativa la seguridad jurídica de los documentos que son enviados y recibidos por medios electrónicos, es real que todas las actuaciones están guiadas bajo leyes que permiten el uso adecuado de las nuevas tecnologías.

> La Constitución de 1991, en concordancia con el artículo 12 de la Declaración Universal de Derechos Humanos, contempla como derechos fundamentales con entidad propia y dimensión bien definida de una parte el derecho a la intimidad, la honra, y en otro aparte, al derecho a la información; sin embargo, algunos de los aspectos que se garantizan en el texto constitucional y convencional, no siempre resultan evidentes y la disposición de este derecho por parte de los individuo ocurre por la falta de información de los propios titulares del derecho sobre la existencia y el potencial de ejercicio del mismo (Corte Constitucional, Art. 7, p. 9).

Bautista (2015) afirma “la disposición inconsciente, en algunos casos, del derecho a la intimidad personal y familiar, en especial con relación al uso masivo de las nuevas tecnologías de la información” (p. 7).

Como expresa Morales (2016) en un párrafo alegando la información antes mencionada:

> La prueba documental digital, es una nueva figura en el campo jurídico, que va evolucionando con las nuevas tecnologías y que requiere ser reglamentada en el campo legal de nuestro ordenamiento jurídico, por su importante valor probatorio, del que se desprenden derechos y obligaciones, que tienen efecto vinculante. La prueba digital ya alcanza un alto porcentaje de equivalente a la prueba física del papel manuscrito del que se predica que sea el original, firmado, integro, autentico y confiable (p. 10).

Por otro lado, Ruíz (2002) afirma “El comercio electrónico se ha establecido como la norma de hacer negocios, basada en una nueva tecnología capaz de automatizar transacciones comerciales asociadas a las empresas mediante mecanismos electrónicos y sin uso del documento basado en papel” (p. 299).

7.1. Ley 527 de 1999

Con el creciente desarrollo del comercio electrónico y los convenios en materia mercantil suscritos por Colombia, fue necesario crear esta ley. Rincón (2008) (citado por Morales, 2016), afirma “En el periodo 30 de sesiones de la CNUDMI, celebrado en 1997, se discutió la viabilidad y conveniencia de preparar un régimen uniforme sobre las cuestiones relativas a las firmas digitales, las entidades certificadoras y asuntos conexos” (p. 11).

Como dice Reyes (2003) (citado por Morales, 2016), “Según se hizo constar en la propia exposición de motivos, el proyecto colombiano se basó en la Ley modelo de la Comisión

de las Naciones Unidas para el 12 desarrollo del Derecho Mercantil Internacional–CNUDMI–sobre Comercio Electrónico" (p. 12).

> Esta ley contiene 47 artículos distribuidos así: Mensajes de datos y comercio electrónico, firmas digitales, certificados y entidades de certificación. En busca de ampliar el concepto de documento a nivel probatorio, que estipula el Artículo 251-Distintas clases de documentos, que regula el Código de Procedimiento Civil (Decreto 1400 de 1970) (p. 12).

Morales (2016) afirma

> Esta ley resalta conceptos del campo tecnológico y conceptos del campo legal, en el que el papel físico era uno de los mayores soportes documentales, ya con el creciente auge de las transacciones electrónicas y una mayor cobertura y accesibilidad al internet, se hacía necesario contar con un soporte documental valido, seguro y confiable que tuviera efectos jurídicos vinculantes y alcance probatorio (p. 12).

7.2. Artículo 28. Atributos jurídicos de la firma digital

De acuerdo con Morales (2016) "Una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo" (p. 14).

"Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:" (Morales, 2016, p. 14).

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Esta bajo el control exclusivo de la persona que la usa.

4. Está ligada a la información o mensaje, de tal manera que, si estos son cambiados, la firma digital es invalidada.
5. Ley 527 (1999) (citado por Morales, 2016) "Esta conforme a las reglamentaciones adoptadas por el Gobierno Nacional" (p. 14).

"La noción de "mensaje" comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación moderna, bajo la configuración de los progresos técnicos que tengan contenido jurídico" (p. 14). Reyes (2003) (citado por Morales, 2016) afirma

> Cuando en la definición de mensaje de datos, se menciona los "medios similares", se busca establecer el hecho de que la norma no está exclusivamente destinada a conducir las practicas modernas de comunicación, sino que pretenden ser útil para involucrar todos los adelantos tecnológicos que se generen en un futuro (p. 14).

7.3. Ley 8 ª de 1970

> En nuestra legislación, podemos evidenciar la regulación entre derecho y tecnología desde el momento que se comienza a utilizar el computador como herramienta en la modernización de la administración pública. Artículo 7º. De acuerdo con el ordinal 12 del artículo 76 de la Constitución Nacional, revístese al Presidente de la Republica de precisas facultades extraordinarias, hasta el 20 de Julio de 1971, para reestructurar la Dirección General de Impuestos Nacionales del Ministerio de Hacienda y Crédito Público y sus oficinas seccionales, fijar las remuneraciones correspondientes y adoptar las medidas necesarias para generalizar el uso del computador electrónico en los trámites administrativos relacionados con los impuestos nacionales y poner especial énfasis en el mejoramiento y organización de las oficinas de Cobranzas y Ejecuciones Fiscales (Morales, 2016, p. 11).

7.4. Ley 794 de 2003

"En la Ley 794 se determina de manera expresa y obligatoria el uso de la firma digital como un mecanismo de aseguramiento técnico y jurídico de las comunicaciones electrónicas en el entorno procesal" (Morales, 2016, p. 17).

Según Peña (2015) "El Consejo Superior de la Judicatura expidió el 2 de marzo de 2006 el Acuerdo PSAAA06-3334 por el cual reglamenta la utilización de medios informáticos y electrónicos en relación con las funciones de Administración de Justicia" (p. 196).

7.5. Ley 906 de 2004

> Con fundamento en la Ley 527 de 1999, se actualizo el Código de Procedimiento Penal, Ley 906 de 2004, en el Articulo 424 – Prueba documental, se incluyó el ítem Mensaje de Datos, dando cobertura al soporte generado por medios electrónicos y de computo, se evidencia un vacío tecnológico en cuanto a los elementos informáticos y tecnológicos que puedan garantizar y brindar certeza sobre la autenticidad, originalidad, confiabilidad e integridad a la información aquí contenida o generada por estos medios, que son desconocidos en el campo jurídico. En el campo de la informática y la tecnología deben tenerse presente los registros que evidencian o registran la creación de dicha información, la preservación de dicha información digital, el almacenamiento digitalizada de dicha información, la consulta de dicha información, los procesos que pueden soportar para ser materializados en listados impresos que puedan ser asimilados por el ser humano, que puedan ser replicados más de una vez, etc (Morales, 2016, p. 19).

7.6. Artículo 424 – Prueba documental

"Para efectos de este código se entiende por documentos los siguientes:" (Morales, 2016, p. 19).

1. Los textos manuscritos, mecanografiados o impresos.
2. Las grabaciones magnetofónicas.
3. Discos de todas las especies que contengan grabaciones.
4. Grabaciones fonópticas o videos.
5. Películas cinematográficas.
6. Grabaciones computacionales.
7. Ley 906 (2004) "Mensajes de datos. …)", citado por (Morales, 2016, p. 20).

7.7. Decreto 2364 de 2012

Expedido por el Ministerio de Comercio, Industria y Turismo el día 22 de noviembre, con el fin de reglamentar el Articulo 7 de la Ley 527 de 1999. La Ley 527 de 1999 dentro de sus disposiciones hace referencia a la firma digital, pero con el creciente auge del comercio electrónico, fue necesario hacer claridad respecto a la neutralidad informática, motivo por el cual en esta disposición se hace referencia a la firma electrónica como esquema alternativo de identificación (Morales, 2016, p. 32).

Artículo 1. Definiciones. Para los fines del presente decreto se entenderá por:

1. Acuerdo sobre el uso de mecanismo de firma electrónica: Acuerdo de voluntades mediante el cual se estipulan las condiciones legales y técnicas a las cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos.
2. Datos de creación de la firma electrónica: Datos únicos y personalísimos, que el firmante utiliza para firmar.
3. Firma electrónica: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

4. Firmante. Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa (Morales, 2016, p. 32).

> Artículo 2. Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para La firma electrónica. Ninguna de las disposiciones del presente decreto será aplicada de modo que excluya, restringa o prive de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el artículo 7 de la Ley 527 de 1999 (Morales, 2016, p. 33).

> Artículo 3. Cumplimiento del requisito de firma. Cuando se exija la firma de una persona, ese requisito quedara cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan confiable como apropiada para los fines con los cuales se generó o comunico ese mensaje (Morales, 2016, p. 33).

Artículo 4. Confiabilidad de la firma electrónica. La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.
2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.

Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona: Demuestre de otra manera que la firma electrónica es confiable

o aduzca pruebas de que una firma electrónica no es confiable (Morales, 2016, p. 33).

"Artículo 5. Efectos jurídicos de la firma electrónica. La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 3 de este decreto" (Morales, 2016, p. 34).

Artículo 6. Obligaciones del firmante. El firmante debe:

1. Mantener control y custodia sobre los datos de creación de la firma.
2. Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma.
3. Dar aviso oportuno a cualquier persona que posea, haya recibido o vaya a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si:
   a. El firmante sabe que los datos de creación de la firma han quedado en entredicho
   b. Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho (Morales, 2016, p. 34).

Decreto 2364 (2012) (citado por Morales, 2016).

> Se entiende que los datos de creación del firmante han quedado en entredicho cuando estos, ente otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma (p. 34).

Conclusión

"Los avances tecnológicos se han vuelto una parte esencial de nuestras vidas. Para entender por qué, solo basta con mirar a nuestro alrededor y ver que en todo momento y contexto estamos rodeados por ella" (Importancia de la tecnología, 2016); ya sea en el área comercial hasta el área ejecutiva, que estemos trabajando o descansando, siempre está presente para hacer nuestras vidas más sencillas.

> La aparición y masificación de los documentos electrónicos a través de las tecnologías ha permitido: reducir el espacio físico de archivo, mantener un único conjunto de información que contenga todo aquello que fue o es importante, posibilitar la localización rápida por una gran diversidad de criterios, facilitar el procesamiento paralelo de información contenida en documentos. Prueba de esto es que actualmente existen diversos modelos teóricos en áreas de la seguridad de información y los documentos electrónicos (García, 2011), como los criptosistemas de clave privada, secreta y pública y la firma digital.

Se dieron a entender diversos factores que perjudicaban la seguridad de jurídica de los documentos electrónicos, entre ellos podemos encontrar los factores de riesgo ambientales como la lluvia, apagones de luz, humedad, tecnológicos tales como fallas de hardware, software o algún ataque por un virus informático y humanos como fraudes, modificaciones en los archivos, robos de contraseña entre otros.

Colombia no aplica con rigurosidad los parámetros de seguridad informática aun teniendo leyes con el objetivo de proteger y garantizar la confidencialidad, integridad y disponibilidad de estos datos, esto significa que solamente cuando estamos conscientes de las potenciales amenazas tecnológicas, podemos tomar medidas de protección adecuadas para que no se pierdan o dañen nuestros recursos valiosos.

El país debe avanzar en miras al uso de las TIC, donde toda la población tenga el derecho fundamental de la educación, tomando en cuenta estos temas de seguridad en los documentos electrónicos para evitar pérdidas de información confiable y confidencial.

Referentes bibliográficos

Alvite Díez, M. L. (2009). Las bases de datos jurídicas y el uso del lenguaje XML en España. *Scire. 15:1 ISSN 1135-3716*, 33-57.

Bautista Avellaneda, M. E. (2015). *El derecho a la intimidad y su disponibilidad pública.* Bogotá, D. C. : JUS Universidad Católica de Colombia.

Becerra León, H. A. (2002). Documento electrónico y título valor electrónico. *NOVUM JUS*, 79-124.

Becerra, J. C., García Vargas, C. B., Sánchez Acevedo, M. E., & Torres Ávila, J. (2015). *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)* . Bogotá: Digiprint editores e. u.

Congreso de Colombia. (18 de Enero de 2011). *Ley 1437 de 2011.* Obtenido de Defensoria: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1437_2011.pdf

Constitución Política de Colombia. (2020). *Artículo 209.* Bogotá, D. C. : Legis Editores S. A. . Obtenido de Leyes.co: https://leyes.co/constitucion/209.htm

Decreto 2364, 2. (2012). *Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.* Bogotá: Presidencia de la República de Colombia.

Díaz García, A. (31 de Marzo de 2010). *Los documentos electrónicos y sus efectos legales en Colombia.* Obtenido de SlideShare: https://es.slideshare.net/alediaganet/los-documentos-electrnicos-y-sus-efectos-legales-en-colombia

Díaz Miranda, M. A. (2006). *TESIS DE GRADO: Seguridad jurídica de los documentos electrónicos.* Obtenido de Repositorio UNIVERSIDAD MAYOR DE SAN ANDRES: https://repositorio.umsa.bo/bitstream/handle/123456789/18854/T-2140.pdf?sequence=1&isAllowed=y

Echeverria Peña, G. L. (2013). *Procedimientos y Medidas de Seguridad Informatica. Conceptos Básicos de Seguridad de Redes.* Guatemala: eBook Tercera Edición.

Formentín Zayas, Y. M. (2013). La firma electrónica, su recepción legal. Especial referencia a la ausencia legislativa en Cuba. *IUS Revista del Institutto de Ciencias jurídicas de puebla, México, ISSN: 1870-2147. Año VII, No. 31*, 104-120.

Función Pública, D. A. (18 de Agosto de 1999). *Ley 527 de 1999.* Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=4276

Granger, S. (19 de Noviembre de 2009). *"Social Engineering Fundamentals, Part I: Hacker Tactics"* . Obtenido de Security Focus: http://www.securityfocus.com/infocus/1527

Henao Restrepo, D. (2000). Ley de Comercio electrónico en Colombia, Ley 527 de 1999 "Nuevos retos del derecho Comercial. *XV Congreso Nacional de derecho comercial, Medellín 1999,*. Medellín: Biblioteca jurídica Diké. .

Huerta Miranda, M., & Líbano Manzur, C. (21 de Noviembre de 2008). *Efectos jurídicos del documento electrónico.* Obtenido de Delitos Informaticos: http://gonzo-stelgon.blogspot.com/2008/11/efectos-jurdicos-del-documento.html

Jiménez, W. G., & Meneses Quintana, O. (2017). Derecho e internet: Introducción a un campo emergente para la investigación y práctica jurídicas. *Revista Prolegómenos Derecho y Valores Volumen XX Número 40 ISSN 0121-182X*, 43-61.

Jovel Sánchez, L. C. (2003). El documento electrónico, la firma digital y la contratación administrativa. *Revista de ciencias jurídicas*, 25-54. Obtenido de Corteidh: https://www.corteidh.or.cr/tablas/a12900.pdf

Ley 527, 1. (1999). *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación.* Bogotá: Congreso de Colombia. Diario Oficial 43.673 de 21 de agosto de 1999.

Ley 906, 2. (2004). *Por la cual se expide el Código de Procedimiento Penal.* Bogotá: Congreso de Colombia. Diario Oficial 45.658 de 1 de septeimbre de 2004.

Maza Márquez, M. (1998). *Manual de Criminalística.* Bogotá: 2° Edición. Editorial Libreria del Profesional.

Medina Torres, C. B. (2001). *Pruebas en Derecho Comercial.* Bogotá, D. C. : 2° Edición, Legis.

Morales Sánchez, F. (2016). *Validez de la prueba electrónica, un estudio sobre la firma digital y electrónica.* Obtenido de Universidad Católica de Colombia:

https://repository.ucatolica.edu.co/bitstream/10983/13779/4/VALIDEZ%20DE%20LA%20PRUEBA%20ELECTRONICA.pdf

Peguera Poch, M., Guilayn, A. A., Casas Vallés, R., Martínez, A. C., Delgado García, A. M., Herrera Joancomartí, J., & Jeffery, M. (2005). *Derecho y nuevas tecnologías.* Barcelona: Editorial UOC.

Peña Valenzuela, D. (2015). *De la firma electrónica y las entidades de certificación. .* Bogotá: Universidad Externado de Colombia.

Pontiroli, S. (29 de Octubre de 2013). *PGP-Privacidad, seguridad y autenticación fiables para todos* . Obtenido de Kaspersky daily: https://www.kaspersky.es/blog/pgp-privacidad-seguridad-y-autenticacion-fiables-para-todos/1781/

Quiroz Zambrano, S. M., & Macías Velancia, D. G. (2017). Seguridad en informática: consideraciones. *Dom. Cien., ISSN: 2477-8818. Vol. 3, núm. 1. ,* 676-688.

Redondo Herranz, M. d. (2010). El documento electrónico: un enfoque archivístico. *Revista General de Información y Documentación*, 391-408.

Rendón López, A. (2009). La seguridad del documento electrónica: Reto jurídico del presente. *Revista AMICUS CURIAE AÑO IV NÚMERO 4 UNAM*, 1-17.

Rengifo García, E. (2000). Comercio electrónico, documento electrónico y seguridad jurídica. *XV Congreso Nacional de derecho comercial, 1999* (pág. 88). Medellín: Biblioteca jurídica Diké.

Rengifo García, E. (2000). *Comercio Electrónico, documento electrónico y Seguridad Jurídica, memorias sobre Comercio Electrónico.* Bogotá, D. C. : Universidad Externado de Colombia, 1° Edición.

Reyes Krafft, A. (2003). *La firma electrónica y las entidades de certificación.* México: Porrua.

Rincón Cárdenas, E. (2008). *Aproximación jurídica a la firma digital y a los prestadores de servicio de certificación digital en la Comunidad Andina de Naciones.* Bogotá: Certicamara.

Rincón Cárdenas, E. (2008). *Aproximación jurídica a la firma digital y a los prestadores de servicio de certificación digital en la Comunidad Andina de Naciones.* Bogotá: Certicamara.

Ruíz García, T. (2002). Firma electrónica y certificación. *Boletín de estudios económicos-Bilbao.57(176)*, 299-310.

Torres Ávila, J. (2015). La fundamentación del derecho a la inclusión digital. *Revista Prolegómenos - Derecho y Valores*, 47-64.

Vallbé, J. J. (2007). *Iuriservice: ontologies per a la representació del coneixement jurídic. // I Congrés Català de Filosofia.* Obtenido de Barcelona: Institut d'Estudis Catalans, 2007.: http://idt.uab.es/docs/2007/Iuriservice-FILCAT.pdf

Velasco Melo, A. H. (2008). El Derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. *Revista de Derecho, Universidad del Norte No. 29 Baranquilla ISSN 0121-8697*, 333-336.

Villalobos Pérez, J. (1990). La Nulidad de los Instrumentos Notariales. *Revista del Colegio de Notarios de Jalisco. Primer Semestre, Gráfica Nueva, Guadalajara Jalisco. Número 119, México.*, 88-130.

Voutssas M, J. (2010). Preservación documental digital y seguridad informática. *Investigación Bibliotecológica ISSN: 2448-8321, Vol. 24 Núm. 50*, 127-155.

Zimmermann, P. (22 de Febrero de 2019). *Seguridad informática PGP*. Obtenido de El rincón del hacker: https://draustico.wordpress.com/2019/02/22/seguridad-informatica-pgp/